

УТВЕРЖДЕН
ПФНА.26.20.40.142.003 31-ЛУ
(взамен ПФНА.501410.002 31-ЛУ)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux



Описание применения

ПФНА.26.20.40.142.003 31
(взамен ПФНА.501410.002 31)

АННОТАЦИЯ

Данный документ выполнен в соответствии с ГОСТ 19.402-78 и распространяется на изделие «Система защиты информации от несанкционированного доступа «Dallas Lock Linux» ПФНА.26.20.40.142.003 (далее по тексту — СЗИ НСД, изделие).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия (далее по тексту — ПО изделия или СЗИ НСД), условиях применения, описание задачи, перечень входных и выходных данных.

СОДЕРЖАНИЕ

1	НАЗНАЧЕНИЕ	4
2	УСЛОВИЯ ПРИМЕНЕНИЯ	5
3	ОПИСАНИЕ ЗАДАЧИ	8
4	ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ	20
	4.1 Входные данные	20
	4.2 Выходные данные	20

1 НАЗНАЧЕНИЕ

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС), иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), при защите значимых объектов критической информационной инфраструктуры (КИИ).

Изделие предназначено для использования на технических средствах (ТС), таких как персональные компьютеры, портативные компьютеры (ноутбуки), серверы и ТС с поддержкой виртуальных сред.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

СЗИ НСД может быть использовано на ТС, работающих под управлением операционных систем семейства Linux (x64).

Поддерживаются такие ОС:

- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- Альт 8 СП релиз 10 версия 2 (Рабочая станция, Сервер);
- Альт Рабочая Станция 9.0¹, 9.1¹, 9.2¹, 10.0, 10.1, 10.2, 10.4, 11;
- Альт Сервер 10, 11;
- Astra Linux Common Edition 2.12.x²;
- Astra Linux Special Edition 1.7, 1.8;
- Debian 10, 11, 12;
- Red Hat Enterprise Linux 7²;
- Ubuntu-desktop 18.04, 20.04;
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- РОСА «КОБАЛЬТ» 7.9 (Рабочая станция, Сервер)²;
- МСВСфера АРМ 9;
- МСВСфера Сервер 9.

СЗИ НСД поддерживает 64-разрядные версии ОС архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).

СЗИ НСД поддерживает следующие типы файловой системы: ext2, ext3, ext4, JFS, ReiserFS.

Директория «/usr» не должна быть на отдельном от корневого каталога «/» разделе ФС (это касается всех дистрибутивов).

Для размещения файлов **СЗИ НСД** требуется 9 Гб пространства на корневом каталоге жесткого диска:

- в каталоге «/boot» (или «/boot/efi») должно быть не менее 300 Мб свободного пространства;
- в каталоге «/dllx» должно быть не менее 530 Мб свободного пространства;
- в каталоге «/dllibckp» должно быть не менее 374 Мб свободного пространства;
- в каталоге «/lib/modules» должно быть не менее 4,2 Гб свободного пространства;
- в каталоге «/tmp» должно быть не менее 3 Гб свободного пространства.

СЗИ НСД успешно устанавливается на автоматизированное рабочее место как с UEFI/GPT, так и с BIOS/MBR на автоматически размеченный жесткий диск (разметка жесткого диска по умолчанию при установке ОС). При условии, что для всех каталогов есть необходимое свободное место.

Минимальный объем оперативной памяти, занимаемый компонентами **СЗИ НСД**, составляет 500 Мб. При высокой интенсивности файловых операций потребление может достигать до 3 Гб.

Минимальная версия ядра Linux – 5.10.246.

Максимальная версия ядра Linux – 6.1.158.

Для обеспечения интеграции с доменом, изделие поддерживает работу со следующими компонентами:

- SSSD 2.6.3 и старше;
- Winbind 4.13.17 и старше;
- Kerberos 5 и старше;
- OpenLDAP 2.6.1 и старше;
- Samba 4 и старше;

¹ Для защиты ТС, работающих под управлением ОС Альт Рабочая Станция 9.0, 9.1, 9.2 необходимо использовать версию изделия 5.8.306.

² Для защиты ТС, работающих под управлением ОС Astra Linux Common Edition (Open) 2.12.x, Red Hat Enterprise Linux 7 и РОСА «КОБАЛЬТ» 7.9 (Рабочая станция, Сервер), необходимо использовать версию изделия 4.6.230.

- FreeIPA 3 и старше.

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети.

Поддерживаемые внешние устройства:

- USB-накопители, внешние жесткие диски, накопители на оптических дисках;
- принтеры;
- беспроводные устройства.

Изделие соответствует требованиям руководящих документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» — по 5 классу защищенности;
- «Требования к средствам контроля съемных машинных носителей информации» (документ утвержден приказом ФСТЭК России № 87 от 28 июля 2014 г.) — по 4 классу защиты;
- «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ;
- «Требования к межсетевым экранам» (документ утвержден приказом № 9 ФСТЭК России от 9 февраля 2016 г.) — по 4 классу защиты;
- «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты» ИТ.МЭ.В4.ПЗ;
- «Требования к системам обнаружения вторжений» (документ утвержден приказом № 638 ФСТЭК России от 6 декабря 2011 г.) — по 4 классу защиты;
- «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ;
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (документ утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 4 уровню доверия.

При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.26.20.40.142.003 ФО), изделие может быть использовано при создании:

- защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- защищенных государственных информационных систем до 1 класса защищенности включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- защищенных информационных систем персональных данных до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- защищенных автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);
- защищенных значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239

- «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»);
- защищенных государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений до 1 класса защищенности включительно (Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»).

3 ОПИСАНИЕ ЗАДАЧИ

Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» ПФНА.26.20.40.142.003 ТУ (ТУ).

Изделие включает в себя следующие функциональные модули:

- система защиты информации от несанкционированного доступа;
- средство контроля съемных машинных носителей информации (далее по тексту — СКН);
- персональный межсетевой экран (далее по тексту — МЭ);
- система обнаружений вторжений (далее по тексту — СОВ);
- средство обнаружения и реагирования (далее по тексту — СОР).

В соответствии с ТУ СЗИ НСД состоит из программного ядра и следующих подсистем:

- подсистема управления пользователями:
 - подсистема идентификации и аутентификации;
 - подсистема контроля сессий;
- подсистема контроля файловой системы:
 - подсистема разграничения доступа к файлам и каталогам;
 - подсистема гарантированной очистки остаточной информации;
 - подсистема контроля целостности;
- подсистема управления питанием;
- подсистема контроля процессов;
- подсистема журналирования и аудита;
- подсистема самотестирования функционала;
- подсистема контроля внешних систем:
 - подсистема контроля разграничения доступа к блочным и беспроводным устройствам;
 - подсистема контроля печати;
- подсистема сигнализации о событиях безопасности;
- подсистема управления использованием СКН подключения;
- подсистема межсетевого экранирования;
- подсистема обнаружения вторжений:
 - подсистема обнаружения и реагирования;
- подсистема восстановления после сбоев.

Ядро системы защиты выполняет основные функции СЗИ НСД:

- обеспечение доступа к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
- обеспечение проверки целостности СЗИ НСД, объектов ФС, программно-аппаратной среды;
- осуществление полной проверки правомочности и корректности администрирования СЗИ НСД;
- осуществление управления подсистемами и обеспечение их взаимодействия.

В соответствии с ТУ модуль изделия ЕЦУ Dallas Lock состоит из программного ядра, графического интерфейса и следующих подсистем:

- подсистема базы данных;
- подсистема репликации;
- подсистема сетевого взаимодействия;
- подсистема управления конфигурацией;
- подсистема преобразования и визуализации данных;
- подсистема аудита;

- подсистема управления деревом доменных объектов;
- подсистема управления учетными записями;
- подсистема управления ролями;
- подсистема управления сетевыми устройствами;
- подсистема управления заданиями модулей СЗИ Dallas Lock;
- подсистема лицензирования;
- подсистема интеграции с Kaspersky Security Center/Kaspersky Endpoint Security;
- подсистема удаленного администрирования;
- подсистема управления аппаратной идентификацией;
- подсистема удаленного развертывания;
- подсистема сбора журналов;

подсистема сбора информации об АРМ.

Система защиты информации от несанкционированного доступа

3.5.1 Подсистема идентификации и аутентификации

- 3.5.1.1 Изделие требует от пользователей идентифицировать себя при запросах на доступ.
- 3.5.1.2 Изделие проверяет подлинность идентификации — осуществляет аутентификацию.
- 3.5.1.3 Изделие располагает данными для проверки идентификации и аутентификации пользователей в информационной системе.
- 3.5.1.4 Изделие препятствует доступу к защищаемым ресурсам неидентифицированными пользователями и пользователями, подлинность идентификации которых при аутентификации не подтвердилась.
- 3.5.1.5 Изделие осуществляет идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.
- 3.5.1.6 В изделии осуществляется управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
- 3.5.1.7 В изделии осуществляется управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации (eToken PRO/Java, 72K, eToken Pro/SC, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite, Рутокен ЭЦП PKI, JaCarta ГОСТ, JaCarta PKI, JaCarta PKI/Flash, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta LT, JaCarta PRO, ESMART Token, ESMART Token ГОСТ, ESMART 64K, электронные ключи Touch Memory) и принятие мер в случае утраты и (или) компрометации средств аутентификации.
- 3.5.1.8 В изделии осуществляется возможность хранения на аппаратном идентификаторе (защита пин-кодом) и считывания из аппаратного идентификатора авторизационных данных пользователей (не распространяется на электронные ключи Touch Memory).
- 3.5.1.9 В изделии осуществляется защита обратной связи при вводе аутентификационной информации посредством замены вводимых знаков специальными символами, не позволяющими однозначно определить вводимые знаки.
- 3.5.1.10 В изделии осуществляется управление (создание, активация, блокирование и уничтожение) учетными записями пользователей, в том числе регистрация новых и уже имеющихся доменных учетных записей пользователей системы.
- 3.5.1.11 В изделии осуществляется разделение полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
- 3.5.1.12 В изделии осуществляется назначение необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
- 3.5.1.13 В изделии реализован ролевой механизм разграничения доступа к администрированию СЗИ НСД.
- 3.5.1.14 В изделии осуществляется ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

- 3.5.1.15 В изделии осуществляется разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты.
- 3.5.1.16 В изделии реализована возможность авторизации доменных (LDAP) пользователей.
- 3.5.1.17 В изделии реализована возможность добавления доменных учетных записей в локальные группы.
- 3.5.1.18 В изделии гарантирована корректная аутентификация при нескольких подключенных аппаратных идентификаторах во время аутентификации.
- 3.5.1.19 В изделии обеспечена работоспособность команд управления аппаратной идентификацией при удаленном подключении администратора информационной безопасности к автоматизированному рабочему месту.
- 3.5.2 Подсистема контроля сессий**
- 3.5.2.1 В изделии возможно блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
- 3.5.2.2 В изделии есть возможность ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя.
- 3.5.2.3 В изделии реализована возможность задавать расписание работы пользователей.
- 3.5.3 Подсистема разграничения доступа к файлам и каталогам**
- 3.5.3.1 Изделие может контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).
- 3.5.3.2 Для каждой пары (субъект — объект) в информационной системе задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу информационной системы (объекту).
- 3.5.3.3 Изделие содержит механизм, реализующий дискреционные правила разграничения доступа.
- 3.5.3.4 Контроль доступа может быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).
- 3.5.3.5 Механизм, реализующий дискреционный принцип контроля доступа, предусматривает возможности санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей информационной системы и списка защищаемых объектов.
- 3.5.3.6 В изделии предусмотрены средства управления, ограничивающие распространение прав на доступ.
- 3.5.3.7 В изделии реализовано осуществление контроля доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа (дискреционный принцип разграничения прав доступа).
- 3.5.4 Подсистема гарантированной очистки остаточной информации**
- 3.5.4.1 Изделие предотвращает доступ субъекту к остаточной информации при первоначальном назначении или при перераспределении внешней памяти.
- 3.5.4.2 В изделии осуществляется очистка (обнуление, обезличивание) освобождаемых областей памяти внешних накопителей и объектов ФС.
- 3.5.5 Подсистема контроля целостности**
- 3.5.5.1 В изделии предусмотрены средства периодического контроля целостности файловой, программной и информационной части СЗИ НСД.
- 3.5.5.2 В изделии осуществляется контроль целостности программного обеспечения, включая программное обеспечение СЗИ НСД.
- 3.5.5.3 В изделии обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ НСД;
 - целостность программной среды проверяется с периодичностью в 10 минут и по команде администратора по рассчитанным контрольным суммам.

- 3.5.5.4 В изделии осуществляется контроль состава технических средств, программного обеспечения и средств защиты информации.
- 3.5.5.5 В изделии осуществляется контроль целостности для объектов файловой системы.
- 3.5.5.6 В изделии реализованы политики контроля целостности программно-аппаратной среды с возможностью их независимого включения/отключения для системных аппаратных компонентов, дисков и USB-устройств.
- 3.5.6 Подсистема управления питанием**
- 3.5.6.1 В изделии реализована возможность выключения и перезагрузки ТС средствами СЗИ НСД.
- 3.5.7 Подсистема контроля процессов**
- 3.5.7.1 В изделии осуществляется идентификация внешних устройств ТС по логическим именам.
- 3.5.7.2 В изделии осуществляется идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.
- 3.5.8 Подсистема журналирования и аудита**
- 3.5.8.1 В изделии осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения АС.
- 3.5.8.2 В изделии осуществляется регистрация выдачи печатных (графических) документов на «твердую» копию.
- 3.5.8.3 В изделии осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.
- 3.5.8.4 В изделии осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.
- 3.5.8.5 В изделии осуществляется регистрация следующих событий:
- использование идентификационного и аутентификационного механизма;
 - запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
 - создание и уничтожение объекта;
 - действия по изменению правил разграничения доступа.
- 3.5.8.6 Изделие регистрирует события безопасности, связанные с выполнением средством контроля съемных машинных носителей информации функций безопасности, и записывать информацию аудита безопасности.
- 3.5.8.7 В изделии осуществляется регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: внешним устройствам ТС, программам, томам, каталогам, файлам, записям, полям записей.
- 3.5.8.8 В изделии реализована возможность определения типов событий безопасности, подлежащих регистрации, и сроков их хранения.
- 3.5.8.9 В изделии реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.
- 3.5.8.10 В изделии осуществляется сбор, запись и хранение информации о событиях безопасности в течение установленного настройками СЗИ НСД времени хранения.
- 3.5.8.11 В изделии реализован экспорт журналов аудита в форматы, используемые для анализа и печати данных (PDF, ODS, XML).
- 3.5.9 Подсистема контроля и разграничения доступа к беспроводным устройствам**
- 3.5.9.1 В изделии реализована возможность задавать ограничение на использование технологий беспроводного доступа.
- 3.5.10 Подсистема контроля печати**
- 3.5.10.1 В изделии возможно управление доступом к устройствам печати.
- 3.5.10.2 В изделии осуществляется контроль за переносом информации на твердую копию посредством контроля доступа к принтерам.
- 3.5.11 Подсистема сигнализации о событиях безопасности**

- 3.5.11.1 В изделии выполняется регистрация и сигнализация о событиях, относящихся к возможным нарушениям безопасности, а также предоставление возможности выборочного ознакомления с информацией о произошедших событиях.

3.5.12 Подсистема самотестирования функционала

- 3.5.12.1 В изделии осуществляется проверка реализации правил разграничения доступа (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными правилами, средства защиты механизма разграничения доступа, санкционированные изменения правил разграничения доступа).
- 3.5.12.2 В изделии осуществляется тестирование идентификации и аутентификации пользователей, а также их средств защиты.
- 3.5.12.3 В изделии осуществляется проверка регистрации событий:
- 3.5.12.3.1 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.1 ТУ.
- 3.5.12.3.2 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.2 ТУ.
- 3.5.12.3.3 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.3 ТУ.
- 3.5.12.3.4 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.4 ТУ.
- 3.5.12.3.5 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.5 ТУ.
- 3.5.12.3.6 Проверка регистрации событий в соответствии с пунктом 1.4.5.9.6 ТУ.
- 3.5.12.3.7 Проверка средств защиты регистрационной информации.
- 3.5.12.3.8 Проверка возможности санкционированного ознакомления с регистрационной информацией.
- 3.5.12.4 В изделии осуществляется проверка работы механизмов, осуществляющих контроль за целостностью СЗИ НСД.
- 3.5.12.5 Компоненты программного ядра СЗИ НСД, как и их совокупность, имеют механизмы самотестирования.

3.5.13 Программное ядро

- 3.5.13.1 В изделии обеспечена поддержка подлинности сетевых соединений (сеансов взаимодействия) между узлами СЗИ НСД.
- 3.5.13.2 В изделии предусмотрена защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.
- 3.5.13.3 В изделии реализовано функциональное ограничение доступа к методам и данным компонент СЗИ НСД.
- 3.5.13.4 В изделии обеспечена строгая синхронизация данных настроек безопасности компонент СЗИ НСД.
- 3.5.13.5 Программное ядро СЗИ НСД предоставляет безопасный доступ к данным посредством делегирования и распределения совокупности прав.
- 3.5.13.6 Программное ядро СЗИ НСД обеспечивает взаимодействие между узлами СЗИ НСД.
- 3.5.13.7 Программное ядро СЗИ НСД обеспечивает защиту регистрируемых данных от их удаления или модификации.
- 3.5.13.8 Компоненты программного ядра предоставляют набор функциональных возможностей для тестов на покрытие исходного кода (верификации).
- 3.5.13.9 При установке изделия без модуля «Система защиты информации от несанкционированного доступа» изделие автоматически:
- исключает возможность управления пользователями операционной системы, при этом обеспечивая сохранение управления пользователями СЗИ;
 - скрывает все неактивные политики.

3.5.14 Средство администрирования

- 3.5.14.1 СЗИ НСД содержит средства выборочного ознакомления с регистрационной информацией.
- 3.5.14.2 В изделии реализован механизм мониторинга (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

- 3.5.14.3 В изделии реализован механизм управления изменениями конфигурации информационной системы и системы защиты (определение типов возможных изменений конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в конфигурацию информационной системы и ее системы защиты информации).
- 3.5.14.4 В изделии реализована возможность экспорта и импорта конфигурации СЗИ НСД:
- импорт файла конфигурации;
 - экспорт файла конфигурации;
 - установка парольной защиты при создании файла конфигурации;
 - разграничение доступа к управлению конфигурацией;
 - регистрация событий, связанных с управлением конфигурацией, в журналах безопасности.
- 3.5.14.5 Программное ядро СЗИ НСД предоставляет механизм просмотра и анализа информации о действиях отдельных пользователей в информационной системе.
- 3.5.14.6 В изделии реализована возможность выполнения удаленного развертывания СЗИ НСД.
- 3.5.14.7 В изделии реализована интеграция с ЕЦУ Dallas Lock. Обеспечивается:
- синхронизация политик, журналов, учетных записей и результатов проверки контроля целостности;
 - выполнение заданий, получаемых с ЕЦУ;
 - управление СКН;
 - управление МЭ, в том числе профилями и фильтрацией;
 - управление СОВ;
 - управление СОР, включая правила автоматического реагирования и индикаторы компрометации (IoC), а также реализована возможность принимать от ЕЦУ правила автоматического реагирования СОР с неограниченным количеством индикаторов компрометации.
 - удаленная регистрация аппаратных идентификаторов;
 - управление контролем подключенных устройств, в том числе конкретными подключенными устройствами;
 - управление заблокированными локальными и доменными учетными записями.
- 3.5.14.8 В изделии реализовано базовое управление и получение информации от приложения Kaspersky Endpoint Security для Linux с помощью СЗИ НСД.
- Обеспечивается:
- отображение информации о приложении Kaspersky Endpoint Security и управление его работой (включение, отключение);
 - просмотр, запуск, остановка выбранных задач Kaspersky Endpoint Security;
 - отображение информации о событиях из приложения Kaspersky Endpoint Security.
- 3.5.15 Средство контроля съемных машинных носителей информации**
- 3.5.15.1 В изделии осуществляется управление и контроль за использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации.
- 3.5.15.2 Изделие контролирует использование интерфейсов ввода (вывода) информации (в т. ч. на съемные машинные носители информации).
- 3.5.15.3 Изделие обеспечивает контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

- 3.5.15.4 В изделии осуществляется разграничение доступа к управлению СКН и режиму выполнения функций безопасности (контроля накопителей) на основе ролей учетных записей пользователей.
- 3.5.15.5 В изделии осуществляется идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных накопителей информации.
- 3.5.15.6 В изделии осуществляется регламентация и контроль использования в информационной системе мобильных технических средств.
- 3.5.15.7 Изделие содержит механизмы генерации временных меток, и (или) происходит синхронизация системного времени в информационной системе.
- 3.5.16 Персональный межсетевой экран**
- 3.5.16.1 Изделие осуществляет фильтрацию по отправителю информации, получателю информации, сетевому трафику и всем операциям перемещения контролируемой МЭ информации сетевого трафика к узлам информационной системы и от них.
- 3.5.16.2 Изделие обеспечивает распространение фильтрации на все операции перемещения через МЭ информации к узлам информационной системы и от них.
- 3.5.16.3 Изделие осуществляет фильтрацию, основанную на следующих атрибутах безопасности субъектов:
- сетевой адрес узла отправителя;
 - сетевой адрес узла получателя.
- 3.5.16.4 Изделие осуществляет фильтрацию, основанную на следующих типах информации:
- сетевой протокол, который используется для взаимодействия;
 - транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии);
 - разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код;
 - разрешенные (запрещенные) протоколы прикладного уровня;
 - разрешенное (запрещенное) прикладное ПО.
- 3.5.16.5 Изделие предоставляет возможность разрешать или запрещать информационный поток, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации.
- 3.5.16.6 Изделие осуществляет фильтрацию пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика.
- 3.5.16.7 Изделие осуществляет проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию.
- 3.5.16.8 Изделие осуществляет проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором МЭ установлены разрешительные или запретительные атрибуты безопасности.
- 3.5.16.9 Изделие осуществляет фильтрацию SSL/TLS трафика.
- 3.5.16.10 Изделие осуществляет автоматическое блокирование источника информации при кратном срабатывании правила МЭ.
- 3.5.16.11 Изделие разрешает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации.
- 3.5.16.12 Изделие запрещает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации.
- 3.5.16.13 В изделии реализована регистрация и учет выполнения проверок информации сетевого трафика.
- 3.5.16.14 Изделие генерирует записи аудита для событий, потенциально подвергаемых аудиту.

- 3.5.16.15 Для администратора МЭ и аудитора реализована возможность читать информацию из записей аудита доступную в соответствии с их полномочиями.
- 3.5.16.16 Изделие предоставляет записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.
- 3.5.16.17 В изделии реализована регистрация в каждой записи аудита следующей информации об атрибутах безопасности:
- дата и время;
 - идентификатор события (ID);
 - информация (детализация);
 - результат;
 - тип события;
 - адрес источника;
 - порт источника;
 - адрес назначения;
 - порт назначения;
 - пользователь.
- Основываясь на данных атрибутах, изделие предоставляет возможность поиска и сортировки данных аудита.
- 3.5.16.18 В изделии реализована регистрация и учет следующих событий:
- запуск и завершение выполнения функций аудита;
 - результаты выполнения проверок информации сетевого трафика;
 - запись нового значения любой изменяемой политики/параметра.
- 3.5.16.19 В изделии реализована возможность идентификации/аутентификации каждого пользователя до разрешения любого действия, выполняемого при посредничестве МЭ от имени этого пользователя.
- 3.5.16.20 В изделии реализована поддержка определенных ролей по управлению МЭ.
- 3.5.16.21 Для администратора МЭ реализована возможность управлять режимом выполнения функций безопасности МЭ.
- 3.5.16.22 Для администратора МЭ реализована возможность управлять данными МЭ, используемыми функциями безопасности МЭ.
- 3.5.16.23 Для администратора МЭ реализована возможность управлять атрибутами безопасности.
- 3.5.16.24 В изделии реализована возможность ведения для каждого типа мест расположения узла с установленным МЭ отдельных профилей проверок.
- 3.5.16.25 В изделии реализована возможность изменения значений по умолчанию, модификации, удаления, добавления следующих данных для администраторов безопасности:
- содержимое правил МЭ;
 - содержимое профилей проверок.
- 3.5.16.26 В изделии реализована возможность модификации содержимого таблиц состояния соединений для администраторов безопасности.
- 3.5.16.27 В изделии реализована возможность модификации перечня используемых политик МЭ для администраторов безопасности.
- 3.5.16.28 В изделии реализована возможность очистки содержимого журналов аудита МЭ для администраторов безопасности.
- 3.5.16.29 Для администратора МЭ реализована возможность изменения области значений профилей проверок.
- 3.5.16.30 В изделии реализована возможность присвоения профилям проверок допустимых значений, таких как:
- профиль проверок для использования внутри информационной системы;
 - профиль проверок для использования за пределами информационной системы и других допустимых профилей проверок.
- 3.5.16.31 Для администратора МЭ реализована возможность изменения области значений информации состояния соединения.
-

- 3.5.16.32 В изделии реализована возможность присвоения информации состояния соединения допустимых значений, таких как:
- установление соединения;
 - использование соединения;
 - завершение соединения.
- 3.5.16.33 В изделии реализована возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения.
- 3.5.16.34 Для администратора МЭ реализована возможность назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для прикладного программного обеспечения (приложений) с целью последующего осуществления фильтрации.
- 3.5.16.35 Для администратора МЭ реализована возможность модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления МЭ фильтрации.
- 3.5.16.36 В изделии реализована возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования.
- 3.5.16.37 В изделии реализована возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ).
- 3.5.16.38 В изделии реализована возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с МЭ средств защиты информации других видов.
- 3.5.16.39 В изделии предоставлена пользователям возможность верифицировать целостность данных.
- 3.5.16.40 В изделии реализована поддержка правил интерпретации данных, получаемых от взаимодействующих с МЭ средств защиты информации других видов.
- 3.5.16.41 В изделии реализована возможность осуществлять выдачу предупреждающих сообщений пользователю МЭ при обнаружении возможного нарушения безопасности.
- 3.5.17 Система обнаружения вторжений**
- 3.5.17.1 Изделие имеет графический интерфейс администрирования.
- 3.5.17.2 В изделии поддерживаются следующие роли для взаимодействия с модулем COB:
- администратор;
 - аудитор;
 - пользователь ОС.
- 3.5.17.3 В изделии обеспечена возможность ассоциировать пользователей с ролями в части администрирования COB.
- 3.5.17.4 В изделии реализовано обновление и (или) загрузка базы решающих правил (сигнатур трафика) COB в ходе фонового обновления сигнатур.
- 3.5.17.5 В изделии предоставляется возможность настраивать источник и регулярность обновлений базы решающих правил (сигнатуры и (или) эвристики) только администраторам.
- 3.5.17.6 В изделии предоставляется возможность модифицировать режим выполнения функций, связанных с внутренним представлением времени, со сбором данных о системе ИТ, их анализом и ответными реакциями только администратору безопасности.
- 3.5.17.7 В изделии реализована возможность определения ограничений следующих данных только администратором безопасности:
- размер хранимых журналов;
 - время блокировки IP-адреса атакующего.
- 3.5.17.8 В изделии предпринимаются следующие действия при достижении или превышении данными COB, установленных в пункте 3.5.18.7 ограничений:
- архивация журналов при превышении размера хранимых журналов;
 - разблокировка IP-адреса атакующего при истечении времени блокировки IP-адреса атакующего.

- 3.5.17.9 Для администратора COB реализована возможность управлять параметрами COB: настраивать значения глобальных параметров COB, действия срабатываний сигнатур и (или) эвристики, протоколирование событий безопасности COB.
- 3.5.17.10 В изделии реализована возможность управления сбором журналов безопасности COB только администратором и аудитором: экспорт, настройка параметров фильтра журналов.
- 3.5.17.11 В изделии реализована возможность выполнять следующие функции по анализу всех полученных данных COB:
- обнаруживать вторжения в режиме, близком к реальному масштабу времени (допускается задержка в 5 секунд) на уровне отдельных хостов (локальных узлов ИС) путем анализа сетевого трафика без потери данных для анализа;
 - обнаруживать вторжения на уровне отдельных хостов (локальных узлов ИС) путем анализа журналов событий ОС и прикладного ПО.
- 3.5.17.12 В изделии обеспечена возможность по результатам анализа фиксировать следующую информацию:
- дату и время, тип события, результат анализа;
 - уровень тревоги, ID сигнатуры, PID, процесс;
 - протокол (механизм), используемый для проведения вторжения;
 - идентификатор субъекта вторжения, идентификатор объекта вторжения.
- 3.5.17.13 В случае обнаружения вторжений и нарушений безопасности, изделие предпринимает следующие действия:
- осуществляет фиксацию факта обнаружения вторжений или нарушений безопасности в журналах аудита;
 - уведомляет администратора безопасности об обнаруженных вторжениях и нарушениях безопасности с помощью визуального отображения соответствующего сообщения в консоли управления;
 - блокирует IP-адрес атакующего в течении заданного времени;
 - применяет изоляцию узла для блокирования DoS/DDoS-атак.
- 3.5.17.14 Обеспечена возможность собирать информацию о сетевом трафике, проходящем через узлы сети:
- информация о сетевых адресах;
 - информация о используемых портах.
- 3.5.17.15 В изделии обеспечена возможность собирать информацию о следующих событиях на узлах сети:
- события, регистрируемые в журналах аудита: ОС, прикладного программного обеспечения;
 - вызов функций;
 - обращение к ресурсам.
- 3.5.17.16 В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием сигнатурных методов, эвристических методов.
- 3.5.17.17 В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика, методах выявления аномалий в действиях пользователя ИС.
- 3.5.17.18 В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов на заданном уровне.
- 3.5.17.19 Изделие имеет механизмы обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня (ICMPv4, ICMPv6, IPv4, IPv6) и транспортного уровня (UDP, TCP) базовой эталонной модели взаимосвязи открытых систем.
- 3.5.17.20 Изделие имеет механизмы локального, удаленного и централизованного администрирования COB.
- 3.5.17.21 Изделие генерирует записи аудита для следующих событий, потенциально подвергаемых аудиту:

- запуск и завершение выполнения функций аудита;
 - все события, потенциально подвергаемые аудиту, на базовом уровне аудита;
 - чтение информации из записей аудита;
 - все модификации режима выполнения функций, связанных со сбором данных о системе ИТ, их анализом и ответными реакциями;
 - все модификации данных СОВ, сигнатур, данных аудита и всех прочих данных СОВ;
 - все события безопасности СОВ;
 - модификация группы пользователей;
 - выполнение и результаты самотестирования компонентов СОВ.
- 3.5.17.22 В изделии реализована возможность предоставления записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.
- 3.5.17.23 В изделии реализована возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.
- 3.5.17.24 Для администратора и аудитора реализована возможность читать информацию из записей аудита, доступную в соответствии с их полномочиями.
- 3.5.17.25 В изделии реализована возможность запрета всем пользователям доступа к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.
- 3.5.17.26 В изделии реализована регистрация в каждой записи аудита следующей информации об атрибутах события безопасности СОВ:
- дата и время;
 - идентификатор события (ID);
 - тип события;
 - результат;
 - пользователь;
 - уровень тревоги;
 - идентификатор сигнатуры (ID сигнатуры);
 - адрес назначения;
 - порт назначения;
 - адрес источника;
 - порт источника;
 - идентификатор процесса (PID);
 - процесс;
 - объект;
 - информация (детализация).
- 3.5.17.27 В изделии предоставляется возможность выполнять поиск, упорядочивание, сортировку данных аудита, основанную на следующих атрибутах:
- дата и время;
 - тип события;
 - пользователь;
 - объект;
 - результат события (успех/отказ).
- 3.5.17.28 В изделии реализована возможность сохранения отфильтрованной информации из журналов после применения фильтрации.
- 3.5.17.29 В изделии реализована возможность архивации (очистки) содержимого журналов аудита СОВ для администраторов.
- 3.5.17.30 В изделии реализована возможность тестирования (самотестирования) правильного выполнения функций безопасности СОВ (срабатывание тестовой сигнатуры), по запросу уполномоченного пользователя (администратора и аудитора).
- 3.5.17.31 Изделие предоставляет возможность уполномоченным пользователям верифицировать целостность данных функций безопасности СОВ.
- 3.5.17.32 В изделии предоставляется возможность уполномоченным пользователям верифицировать целостность программного кода функций безопасности СОВ.

- 3.5.17.33 В изделии реализован контроль целостности базы решающих правил COB (сигнатур журналов, трафика).
- 3.5.17.34 В изделии реализована возможность настройки автоматического реагирования COB на срабатывание сигнатур и/или эвристик.
- 3.5.17.35 В изделии реализована функциональная возможность «Безопасная среда COB», позволяющая запускать любое стороннее ПО, совместимое с linux-дистрибутивом, в изолированной защищенной среде без внесения изменений в основную ОС, проверять ПО на опасные действия с целью определения степени доверия к нему, формировать отчет о деятельности программы и защищать пользовательские данные от воздействия нежелательного ПО. Отчет создается с правами доступа, исключающими возможность редактирования файла. В отчете отображено следующее:
- общая информация: путь к файлу, аргументы запуска, текущий статус выполнения и код возврата;
 - журналы активности: логи стандартных потоков вывода и ошибок, информация об открытых файлах, сетевых подключениях, системных вызовах и событиях безопасности.
- 3.5.17.36 В изделии, в рамках функциональной возможности «Безопасная среда COB», в отчете реализована классификация опасных событий ядра Linux с соответствующей цветовой индикацией в зависимости от уровня опасности.
- 3.5.18 Средство обнаружения и реагирования**
- 3.5.18.1 В изделии предусмотрена предустановленная база IoC-объектов³ с возможностью ручного и регулярного обновления.
- 3.5.18.2 В изделии реализован механизм обнаружения IoC на автоматизированном рабочем месте по запросу уполномоченного лица.
- 3.5.18.3 В изделии реализована возможность просмотра, активации, деактивации и поиска объектов в базе IoC-объектов.
- 3.5.18.4 В изделии реализована регистрация следующих событий, связанных с индикаторами компрометации:
- изменение списка IoC-объектов (активация и деактивация);
 - обновление базы IoC-объектов;
 - изменение значений политик, связанных с индикаторами компрометации;
 - обнаружение IoC.
- 3.5.18.5 В изделии реализована возможность управления правилами автоматического реагирования COP на обнаружение индикаторов компрометации, в том числе создание, удаление, просмотр, копирование, редактирование, активация, деактивация и изменение приоритета.
- 3.5.18.6 Изделие выполняет одно из следующих действий при срабатывании условий правила автоматического реагирования COP:
- блокировка IP-адреса;
 - блокировка учетной записи;
 - блокировка автоматизированного рабочего места;
 - выключение автоматизированного рабочего места;
 - изоляция узла;
 - журналирование инцидента (срабатывание сигнатуры/эвристики).
- 3.5.18.7 В изделии реализована регистрация следующих событий, связанных с правилами автоматического реагирования COP:
- редактирование списка правил автоматического реагирования COP;
 - изменение значений политик, связанных с правилами автоматического реагирования COP;
 - срабатывание правил автоматического реагирования COP.

³ IoC-объект — JSON-объект, который содержит описание индикатора компрометации. Индикаторы компрометации (IoC) — цифровые артефакты, которые с большой долей вероятности указывают на несанкционированный доступ к системе (то есть ее компрометацию).

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные данные

Входными данными являются:

- файлы конфигураций модулей системы, используемые при установке;
- уникальные для каждого пользователя логин, пароль и серийный номер аппаратного идентификатора;
- сертификаты X.509 для авторизации и верификации компонентов и узлов **СЗИ НСД**;
- формализованные правила политик безопасности, реализуемые с помощью механизмов **СЗИ НСД** и преобразованные в значения атрибутов и полномочий;
- команды управления **СЗИ НСД**;
- сетевой трафик (для **МЭ**, **СОВ**);
- объекты, в которых ведется поиск индикаторов компрометации (для **СОР**);
- установленные соединения (для **МЭ**);
- события, регистрируемые в журналах аудита ОС и приложений (для **СОВ** и **СОР**).

Логин пользователя начинается со строчной буквы или символа подчеркивания и состоит из строчных латинских букв, цифр, символов «_» и «-» введенных с клавиатуры, а также может заканчиваться символом «\$». Длина логина от 2 до 32 символов.

Паролем может служить набор любых символов (длиной от 1 до 30), введенных с клавиатуры.

Минимальная длина и состав символов пароля регулируются соответствующими параметрами безопасности в **СЗИ НСД**.

Выходные данные

Выходными данными являются:

- сообщения **СЗИ НСД** на действия пользователей;
- журналы событий, создаваемые **СЗИ НСД** в процессе работы;
- значения контрольных сумм объектов, на которые установлен контроль целостности;
- резервные копии программных компонентов **СЗИ НСД**;
- файлы конфигураций модулей системы;
- изменения в конфигурационных файлах ОС;
- данные отчетов в результате автоматического тестирования функционала;
- резервные копии объектов, создаваемые при назначении администратором информационной безопасности контроля целостности на объекты ФС.

В журналах событий отслеживаются и соответственно отображаются такие данные, как дата и время, имя пользователя, имя объекта, тип операции, результат попытки доступа, характер ошибки и прочее.